

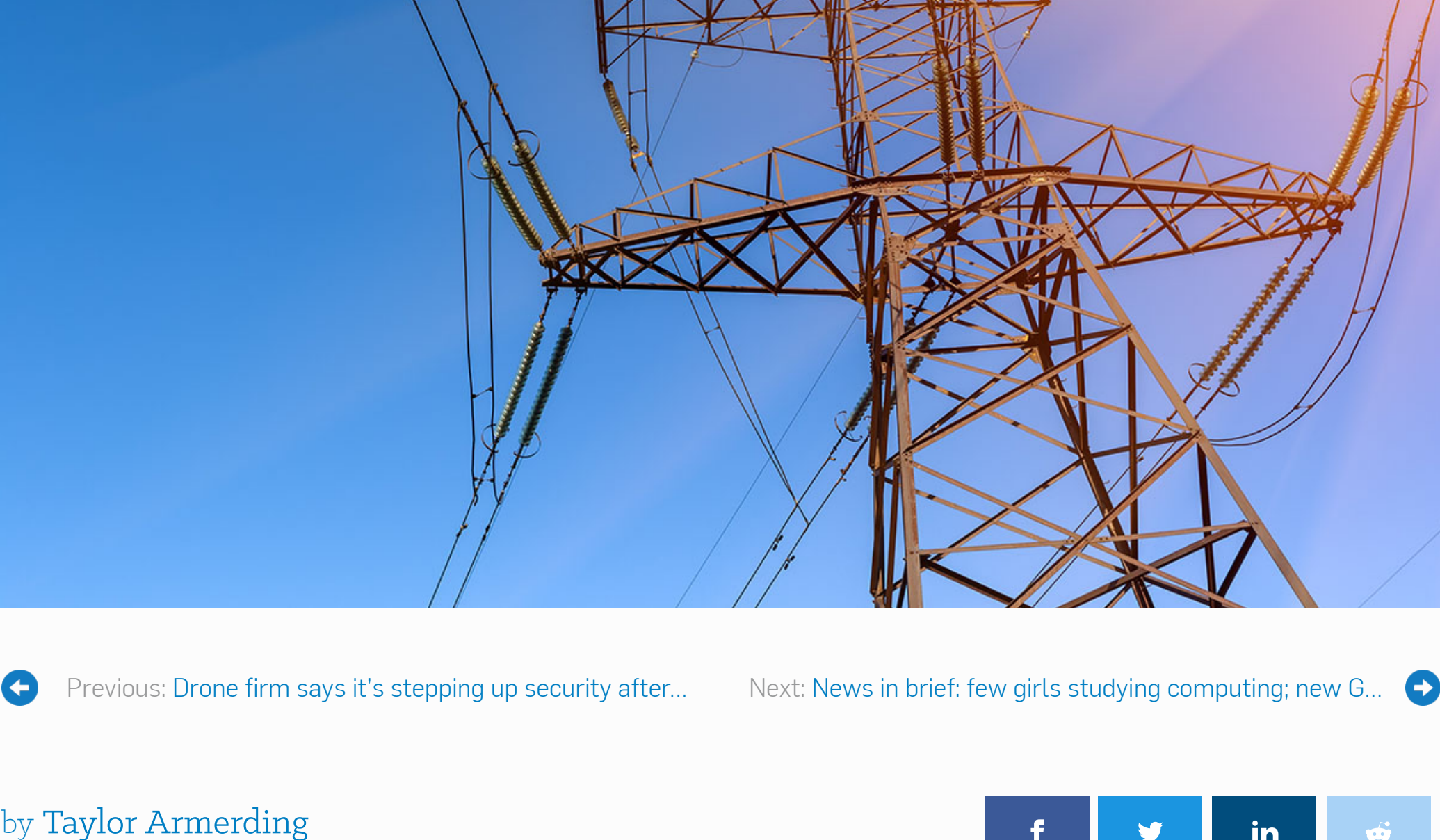
# How likely is a ‘digital Pearl Harbor’ attack on critical infrastructure?

18 AUG 2017 

critical infrastructure, Malware, Ransomware, Security threats

Get the latest security news in your inbox.

Subscribe



 Previous: [Drone firm says it's stepping up security after...](#) Next: [News in brief: few girls studying computing; new G...](#) 

by [Taylor Armerding](#)    

It's coming on two decades now since the first warnings that US critical infrastructure is vulnerable to a catastrophic cyberattack. According to some experts, it is perhaps more vulnerable now than ever – the threats are worse and the security is no better.

But how likely is such an attack? There is still plenty of debate about that.

Richard A Clarke, who in 2000 was the US's top counter-terrorism and cybersecurity chief, gets credit for coining the term "digital Pearl Harbor". He [said at the time](#) that it was "improbable," but added that "statistically improbable events can occur".

There have been similar warnings since from top government officials – former defense secretary [Leon Panetta paraphrased Clarke in 2012](#), warning of a "cyber Pearl Harbor" – a major cyberattack on industrial control systems (ICS) that could disable the nation's power grid, transportation system, financial industry and government for months or longer.

Of course, nothing even close to that catastrophic level has happened – yet. And there are a number of experts who say such doomsday language is gross hyperbole, peddling nothing but FUD (fear, uncertainty and doubt). Marcus Sachs, CSO of the North American Electric Reliability Corporation (NERC), said at the 2015 RSA conference that [squirrels and natural disasters were a more realistic threat of taking down the grid](#) than a cyber attack.

But a couple of experts in ICS – the equipment used to operate the grid and other critical infrastructure – say they are increasingly troubled that security has not really improved since the warnings began.

"With Sophos we've had zero ransomware infections"

Start a 30 day free trial of Sophos Intercept X Endpoint in less than 2 minutes.

Download a free trial

Galina Antova, co-founder and chief business development officer at Claroty, recently referred in a blog to "[The Lost Decade of Information Security](#)", saying:

*"We are no better off today in terms of cybersecurity readiness than we were 10 years ago. The threat landscape is clearly growing more active and dangerous by the day. The theoretical is becoming reality and, unfortunately, we aren't prepared to counter the threat just over the horizon."*

She has some company in the person of Joe Weiss, managing partner at Applied Control Solutions, who has said for years that ICS security is dangerously lax. Writing on his "Unfettered" blog last week, Weiss said there is [essentially no security in ICS process sensors](#), the tools to detect anomalies in the operation of ICSs – which means an attacker could get control of them relatively easily and create major physical damage.

Weiss cited a number of sensor "malfunctions" that illustrate the problem. One, he said, resulted in the release of 10m gallons of untreated wastewater. Another, he said, was the [rupture of a pipeline in Bellingham, WA](#), which released 237,000 gallons of gasoline into a nearby creek causing it to catch fire, killed three people, caused an estimated \$45m in property damage and led to the bankruptcy of the Olympic Pipeline Company.

"That happened in June, 1999," Weiss said in an interview. "How can that be relevant today? It turns out every bit of it is, because the same flaws that existed then exist today."

He said in most cases there is no way to know if what happened was an accident or a malicious attack, because of a lack of visibility into the networks. And he wondered on his blog: "How can this lack of security and authentication of process sensors be acceptable?"

What to do? That is where Weiss and Antova part company – just a bit. Antova said she agrees that the sensor flaws exist and, as she wrote, the threat of major ICS attacks "is real and just over the horizon". But, in an interview, she also said she is "allergic" to describing the threat at either extreme – in relatively trivial terms (squirrels) or disaster (Pearl Harbor).

She said it is not simple or quick to fix flaws in sensors. "Engineers know it takes years to design," she said, "and it can take 25 to 35 years to replace the architecture" of ICS equipment. She ought to know – she was formerly global head of industrial security services at Siemens, a leading manufacturer of power generation and transmission systems.

In her blog post, she said called for implementing what is practical and feasible – the kind of "security hygiene" steps that would keep ICS from being the "low-hanging fruit" that it is now. Things like patches, really taking network segmentation seriously, and giving IT professionals visibility into the networks.

What has hampered that, she wrote, has been a failure to "bridge the gap" between IT and engineering staff, each of whom, "approach the world with different viewpoints, backgrounds and missions." Engineers, she noted, focus on keeping things physically safe and running. Anything that impedes that, they reject.

She also said government regulatory frameworks and standards are, in many cases, not practical. One example she cited was the push for "air-gapped" networks. It sounded good, she said, but it interfered too much with efficiency and the needs of the business. "As a result, air gaps now have one thing in common with unicorns – they don't exist," she wrote.



But just doing security basics would help. "You have to start somewhere," she said.

Weiss contends it is possible, and necessary, to be both more aggressive and creative. Part of the problem, he said, "is a failure of imagination. When you look at the bad guys, they really are bad guys. We need to think like bad guys."


But the two agree that there needs to be better communication between operations and IT. "We've got to have engineering in the same room when IT comes in and says this is what I want to do," Weiss said. "Every time there's an important meeting in DC on cybersecurity, GE and Siemens aren't there."

And both agree that the risk of something really serious happening is growing. "We know these (ICS) networks are exposed," Antova said. "They are resilient and have safety measures, but for a skilled hacker, it's not that hard to fool safety equipment."

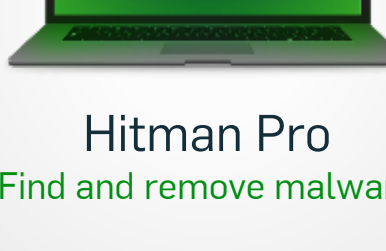
The real menace, she is said, is that ransomware like [WannaCry](#) and [Petya](#) are not just in the hands of nation states, but, "in the hands of every crazy person. I don't think people realize how poor the cyber hygiene is."

 Follow [@NakedSecurity](#) on Twitter for the latest computer security news.  
 Follow [@NakedSecurity](#) on Instagram for exclusive pics, gifs, vids and LOLs!

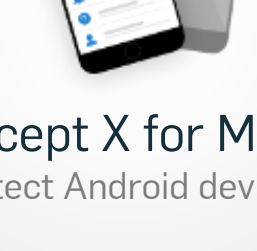
## Free tools



Sophos Home  
Protect personal PCs and Macs




Hitman Pro  
Find and remove malware



Intercept X for Mobile  
Protect Android devices

 Previous: [Drone firm says it's stepping up security after...](#) Next: [News in brief: few girls studying computing; new G...](#) 

## One comment on “How likely is a ‘digital Pearl Harbor’ attack on criti...






Tim Boddington

August 18, 2017 at 8:57 pm

Truly frightening. That engineers are using IT and networking capabilities without a full understanding of the threats and risks involved and taking appropriate contermasures sounds like culpable negligence to me. It's time someone pointed out to managements what their responsibilities include and where the buck stops when it all goes belly up.

I retired as a head of security 22 years ago. It troubles me that the general standard of security appears not to be even as good as the poor security we had in the mid 1990s.

 2  0  Rate This

Reply

## What do you think?

Comment

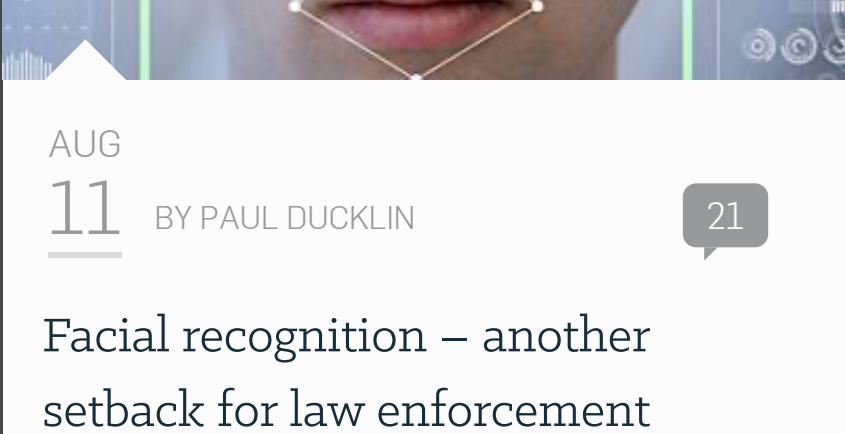
Name

Email

Website

Post Comment

## Recommended reads

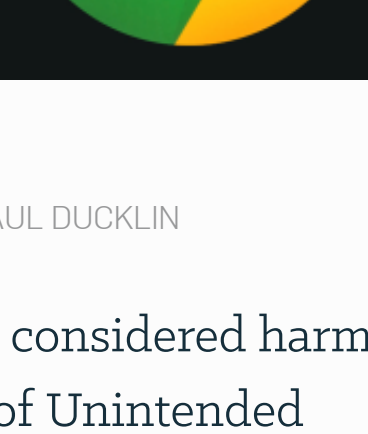


AUG 11

BY PAUL DUCKLIN

21

Facial recognition – another setback for law enforcement

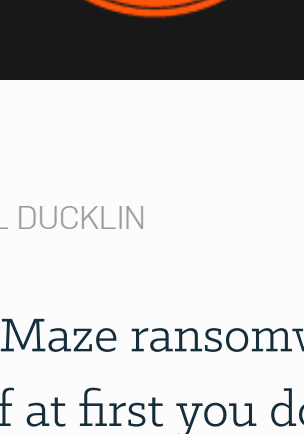


AUG 26

BY PAUL DUCKLIN

28

"Chrome considered harmful" – the Law of Unintended Consequences



SEP 18






BY PAUL DUCKLIN

4

A real-life Maze ransomware attack – "If at first you don't succeed..."

SOPHOS

About Naked Security | Intercept X | XG Firewall | Managed Threat Response  
Send us a tip | Intercept X for Server | Sophos Email | Cloud Optim  
Privacy | Intercept X for Mobile | Sophos Wireless | Phish Threat  
Legal

© 1997 - 2020 Sophos Ltd. All rights reserved. Powered by [WordPress](#) com VIP